



CVE-2009-2700

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2009-2700
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-09-02 17:30:00 UTC
Updated	2021-06-16 12:43:00 UTC
Description	src/network/ssl/qsslcertificate.cpp in Nokia Trolltech Qt 4.x does not properly handle a '\0' character in a domain name in the

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Digia	Qt	4.0.0	All	All	All
Application	Digia	Qt	4.0.1	All	All	All
Application	Digia	Qt	4.1.0	All	All	All
Application	Digia	Qt	4.1.1	All	All	All
Application	Digia	Qt	4.1.2	All	All	All
Application	Digia	Qt	4.1.3	All	All	All
Application	Digia	Qt	4.1.4	All	All	All
Application	Digia	Qt	4.1.5	All	All	All
Application	Digia	Qt	4.2.0	All	All	All
Application	Digia	Qt	4.2.1	All	All	All
Application	Digia	Qt	4.2.3	All	All	All
Application	Digia	Qt	4.3.0	All	All	All
Application	Digia	Qt	4.3.1	All	All	All
Application	Digia	Qt	4.3.2	All	All	All
Application	Digia	Qt	4.3.3	All	All	All
Application	Digia	Qt	4.3.4	All	All	All
Application	Digia	Qt	4.3.5	All	All	All

Application	Digja	Qt	4.4.0	All	All	All
Application	Digja	Qt	4.4.1	All	All	All
Application	Digja	Qt	4.4.2	All	All	All
Application	Digja	Qt	4.4.3	All	All	All
Application	Digja	Qt	4.5.0	All	All	All
Application	Digja	Qt	4.5.1	All	All	All
Application	Digja	Qt	4.5.2	All	All	All
Application	Digja	Qt	4.5.3	All	All	All
Application	Digja	Qt	4.6.0	All	All	All
Application	Digja	Qt	4.6.0	rc1	All	All
Application	Digja	Qt	4.6.1	All	All	All
Application	Digja	Qt	4.6.2	All	All	All
Application	Digja	Qt	4.6.3	All	All	All
Application	Digja	Qt	4.6.4	All	All	All
Application	Digja	Qt	4.7.0	All	All	All
Application	Digja	Qt	4.7.1	All	All	All
Application	Digja	Qt	4.7.2	All	All	All
Application	Digja	Qt	4.7.3	All	All	All
Application	Digja	Qt	4.7.4	All	All	All
Application	Digja	Qt	4.7.5	All	All	All
Application	Digja	Qt	4.8.0	All	All	All
Application	Digja	Qt	4.8.1	All	All	All
Application	Digja	Qt	4.8.2	All	All	All
Application	Digja	Qt	4.8.3	All	All	All
Application	Digja	Qt	4.8.4	All	All	All
Application	Digja	Qt	4.0.0	All	All	All
Application	Digja	Qt	4.0.1	All	All	All
Application	Digja	Qt	4.1.0	All	All	All
Application	Digja	Qt	4.1.1	All	All	All
Application	Digja	Qt	4.1.2	All	All	All
Application	Digja	Qt	4.1.3	All	All	All
Application	Digja	Qt	4.1.4	All	All	All
Application	Digja	Qt	4.1.5	All	All	All
Application	Digja	Qt	4.2.0	All	All	All
Application	Digja	Qt	4.2.1	All	All	All

Application	Digia	Qt	4.2.3	All	All	All
Application	Digia	Qt	4.3.0	All	All	All
Application	Digia	Qt	4.3.1	All	All	All
Application	Digia	Qt	4.3.2	All	All	All
Application	Digia	Qt	4.3.3	All	All	All
Application	Digia	Qt	4.3.4	All	All	All
Application	Digia	Qt	4.3.5	All	All	All
Application	Digia	Qt	4.4.0	All	All	All
Application	Digia	Qt	4.4.1	All	All	All
Application	Digia	Qt	4.4.2	All	All	All
Application	Digia	Qt	4.4.3	All	All	All
Application	Digia	Qt	4.5.0	All	All	All
Application	Digia	Qt	4.5.1	All	All	All
Application	Digia	Qt	4.5.2	All	All	All
Application	Digia	Qt	4.5.3	All	All	All
Application	Digia	Qt	4.6.0	All	All	All
Application	Digia	Qt	4.6.0	rc1	All	All
Application	Digia	Qt	4.6.1	All	All	All
Application	Digia	Qt	4.6.2	All	All	All
Application	Digia	Qt	4.6.3	All	All	All
Application	Digia	Qt	4.6.4	All	All	All
Application	Digia	Qt	4.7.0	All	All	All
Application	Digia	Qt	4.7.1	All	All	All
Application	Digia	Qt	4.7.2	All	All	All
Application	Digia	Qt	4.7.3	All	All	All
Application	Digia	Qt	4.7.4	All	All	All
Application	Digia	Qt	4.7.5	All	All	All
Application	Digia	Qt	4.8.0	All	All	All
Application	Digia	Qt	4.8.1	All	All	All
Application	Digia	Qt	4.8.2	All	All	All
Application	Digia	Qt	4.8.3	All	All	All
Application	Digia	Qt	4.8.4	All	All	All
Application	Qt	Qt	4.0.0	All	All	All
Application	Qt	Qt	4.0.1	All	All	All
Application	Qt	Qt	4.1.0	All	All	All
Application	Qt	Qt	4.1.1	All	All	All

Application	Qt	Qt	4.1.1	All	All	All
Application	Qt	Qt	4.1.2	All	All	All
Application	Qt	Qt	4.1.3	All	All	All
Application	Qt	Qt	4.1.4	All	All	All
Application	Qt	Qt	4.1.5	All	All	All
Application	Qt	Qt	4.2.0	All	All	All
Application	Qt	Qt	4.2.1	All	All	All
Application	Qt	Qt	4.2.3	All	All	All
Application	Qt	Qt	4.3.0	All	All	All
Application	Qt	Qt	4.3.1	All	All	All
Application	Qt	Qt	4.3.2	All	All	All
Application	Qt	Qt	4.3.3	All	All	All
Application	Qt	Qt	4.3.4	All	All	All
Application	Qt	Qt	4.3.5	All	All	All
Application	Qt	Qt	4.4.0	All	All	All
Application	Qt	Qt	4.4.1	All	All	All
Application	Qt	Qt	4.4.2	All	All	All
Application	Qt	Qt	4.4.3	All	All	All
Application	Qt	Qt	4.5.0	All	All	All
Application	Qt	Qt	4.5.1	All	All	All
Application	Qt	Qt	4.5.2	All	All	All
Application	Qt	Qt	4.5.3	All	All	All
Application	Qt	Qt	4.6.0	All	All	All
Application	Qt	Qt	4.6.0	rc1	All	All
Application	Qt	Qt	4.6.1	All	All	All
Application	Qt	Qt	4.6.2	All	All	All
Application	Qt	Qt	4.6.3	All	All	All
Application	Qt	Qt	4.6.4	All	All	All
Application	Qt	Qt	4.7.0	All	All	All
Application	Qt	Qt	4.7.1	All	All	All
Application	Qt	Qt	4.7.2	All	All	All
Application	Qt	Qt	4.7.3	All	All	All
Application	Qt	Qt	4.7.4	All	All	All
Application	Qt	Qt	4.7.5	All	All	All
Application	Qt	Qt	4.8.0	All	All	All
Application	Qt	Qt	4.8.1	All	All	All

Application	Qt	Qt	4.8.2	All	All	All
Application	Qt	Qt	4.8.3	All	All	All
Application	Qt	Qt	4.8.4	All	All	All

References

Reference	Source	Link
Ubuntu update for qt - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.c
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vup
Qt NULL Character CA SSL Certificate Validation Security Bypass Vulnerability	BID	www.sec
Support / Security / Advisories // MDVSA-2009:225 Mandriva	MANDRIVA	www.ma
USN-829-1: Qt vulnerability Ubuntu	UBUNTU	www.ubu
Qt NULL Character Certificate Spoofing Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	secunia.c
Commit in qt in Qt - Qt by Nokia	CONFIRM	qt.gitorio
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-09-03	Tomas Hoger	Not vulnerable. This issue did not affect the versions of qt and qt4 as shipped with Red Hat Ent

There are currently no legacy QID mappings associated with this CVE.

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)